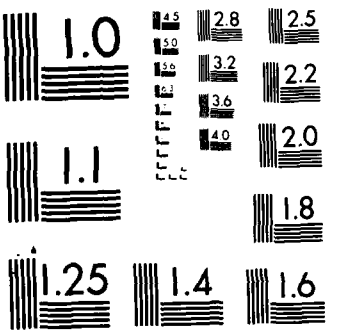
AD-A159 236 TECHNIQUES FOR THE DESIGN AND IMPLEMENTATION OF HIGHLY RELIABLE MULTI-PROCESSING SYSTEMS(U) STANFORD UNIV CA D C LUCKHAM 10 MAY 85 AFOSR-TR-85-0693 AFOSR-83-0355 1/1

UNCLASSIFIED F/G 9/2 NL



MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS 1963 A

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE

AD-A159 236

2

REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION: UNCLASSIFIED	1b. RESTRICTIVE MARKINGS
2a. SECURITY CLASSIFICATION AUTHORITY	3. DISTRIBUTION/AVAILABILITY OF REPORT: Approved for public release; distribution unlimited.
2b. DECLASSIFICATION/DOWNGRADING SCHEDULE	
4. PERFORMING ORGANIZATION REPORT NUMBER(S)	5. MONITORING ORGANIZATION REPORT NUMBER(S): AFOSR-TR- 85-0613
6a. NAME OF PERFORMING ORGANIZATION: Stanford University; 6b. OFFICE SYMBOL (If applicable)	7a. NAME OF MONITORING ORGANIZATION: Air Force Office of Scientific Research
6c. ADDRESS (City, State and ZIP Code): Stanford, CT	7b. ADDRESS (City, State and ZIP Code): Directorate of Mathematical & Information Sciences, Bolling AFB DC 20332-6448
8a. NAME OF FUNDING/SPONSORING ORGANIZATION: AFOSR; 8b. OFFICE SYMBOL (If applicable): NM	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER: AFOSR-83-0355
8c. ADDRESS (City, State and ZIP Code): Bolling AFB DC 20332-6448	10. SOURCE OF FUNDING NOS.

PROGRAM ELEMENT NO.	PROJECT NO.	TASK NO.	WORK UNIT NO.
61102F	2304	A2	

11. TITLE (Include Security Classification): Techniques for the Design and Implementation of Highly Reliable Multi-processing Systems

12. PERSONAL AUTHOR(S): Luckham

13a. TYPE OF REPORT	13b. TIME COVERED	14. DATE OF REPORT (Yr., Mo., Day)	15. PAGE COUNT
Annual	FROM 30 Sep 84 TO 1 Aug 85	10 May 1985	6

16. SUPPLEMENTARY NOTATION

17. COSATI CODES			18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
FIELD	GROUP	SUB. GR.	
XXX	XXXXXXXXXXXXX		

19. ABSTRACT (Continue on reverse if necessary and identify by block number)

During this research period several significant accomplishments were obtained. The completion of implementation of a prototype runtime monitor for detecting deadness errors in Ada tasking was accomplished. The work on runtime monitoring for deadness errors was presented at the IEEE Ada Conference in October 1984, and an invited publication appeared in IEEE Software in March 1985. A new language, called TSL (for Task Sequencing Language) to be used for specifying Ada tasking behavior, was designed and presented at the International Ada Conference in May 1985.

DTIC FILE COPY

DTIC ELECTE SEP 13 1985 D

20. DISTRIBUTION/AVAILABILITY OF ABSTRACT	21. ABSTRACT SECURITY CLASSIFICATION
UNCLASSIFIED/UNLIMITED ☒ SAME AS RPT. ☐ DTIC USERS ☐	UNCLASSIFIED

22a. NAME OF RESPONSIBLE INDIVIDUAL	22b. TELEPHONE NUMBER (Include Area Code)	22c. OFFICE SYMBOL
John P. Thomas, Jr	(202) 767- 5026	NM

DD FORM 1473, 83 APR EDITION OF 1 JAN 73 IS OBSOLETE.

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE

Accession For
NTIS GRA&I
DTIC TAB
Unannounced
Justification
By
Distribution/
Availability Codes
Avail and/or
Dist Special
A-1

10 May 1985

Captain John Thomas
AFOSR/NM
Bolling Air Force Base
Washington, D.C. 20332

Dear Captain Thomas:

Regarding: Grant AFOSR-83-0355 *"Techniques for the Design and Implementation of Highly Reliable Multi-Processing Systems"*.

Enclosed is a short outline of our work and progress under grant AFOSR-83-0355 during the current year. Also included is a short proposal and budget for the continuation of our work in the coming year, September 30, 1985 - September 29, 1986. The budget is based on the third year budget included with the orginal four-year proposal approved by AFOSR in August, 1983. There are minor differences due to the changes in Stanford's personnel costs.

The following enclosed papers, reports, and implementation design study, were sponsored by AFOSR during the period September 30, 1984 through September 29,1985 under Grant AFOSR-83-0355.

A. **Papers.**

These papers were published during the current year's work in refereed conference proceedings or technical journals. One of the papers was invited for publication in a special issue of IEEE Software.

1. *"Debugging Ada Tasking Programs"*, by David P. Helmbold and David C. Luckham, published in the Proceedings of the IEEE Computer Society 1984 Conference on Ada Applications and Environments, pp.96-105 (ISBN 0-8186-0590-1) St.Paul, Minnesota, October 15-18, 1984.

2. *"Debugging Ada Tasking Programs"*, by David P. Helmbold and David C. Luckham, invited paper for a special issue of IEEE Software, IEEE Software, Volume 2, Number 2, pp.47-57 (ISSN 0740-7459) March, 1835.

3. *"TSL: Task Sequencing Language"*, by David P. Helmbold and David C. Luckham, to be presented 1985 Ada International Conference, Paris, France, May 14-16th, 1985.

4. *"Runtime Detection and Description of Deadness Errors in Ada Tasking"*, by David P. Helmbold and David C. Luckham, Ada Letters, Volume IV, Number 6, pp.60-72, May-June, 1985.

B. **Technical Reports.**
The following technical reports were also sponsored under the AFOSR Grant. The reports include full details of prototype implementations and examples. It is generally not possible to publish the complete details of these reports in conference proceedings or technical journals because of space limitations.

1. *"Runtime Detection and Description of Deadness Errors in Ada Tasking"*, by David P. Helmbold and David C. Luckham, Stanford University, Computer Systems Laboratory Technical Report 83-249, November, 1983.

2. *"Debugging Ada Tasking Programs"*, by David P. Helmbold and David C. Luckham, Stanford University, Computer Systems Laboratory Technical Report 84-262, July, 1984.

C. **Draft Documents** of work currently in Progress under AFOSR sponsorship.

1. *"Preliminary Design of a Runtime TSL Monitor"* by Doug Bryan, Computer Systems Laboratory, Stanford University.

D. **Related Work** by this research group that is currently being used in the TSL implementation.

1. *"An Overview of Anna, A Specification Language for Ada"* by David C. Luckham and Friedrich von Henke, Stanford University, Computer Systems Laboratory Technical Report 84-265, September, 1984.

2. *"A Methodology for the Design of Ada Transformation Tools in a DIANA Environment."* by David S. Rosenblum, IEEE Software, Volume 2, Number 2 pp.23-33, (ISSN 0740-7459) March, 1985.

Yours sincerely,

David C. Luckham
Professor of Electrical
Engineering (Research)

Research Progress Report and Proposal
under
AFOSR Grant-83-0355

Techniques for the Design and Implementation
of
Highly Reliable Multi-Processing Systems

Principle Investigator: David C. Luckham

1 Progress in 1984 - 1985.

This is the second year of Grant AFOSR-83-0355. It has been both a consoldiation year and a break-through year. Main accomplishments this year are:

- Completion of implementation of a prototype runtime monitor for detecting deadness errors in Ada tasking, and reports detailing implementation.
- Presentation of the work on runtime monitoring for deadness errors at the IEEE Ada conference, October 1984, and invited publication in IEEE Software in March 1985.
- Design of TSL, a new language for specifying Ada tasking behavior.
- Presentation of TSL at the International Ada conference, Paris, May 1985.

During this year work has been completed on runtime monitoring for *deadness* errors. The basic principles of detecting deadness errors in Ada tasking were applied in the implementation of a prototype runtime monitor. This was successfully demonstrated on example tasking programs. Design principles used in the Ada implementation of the monitor were defined; as a result, runtime monitors developed by this work are extensible and reusable.

This work was published in two reports and three papers. It was presented at the IEEE Ada Conference in October 1984. Subsequently this work was invited for a special issue of IEEE Software on Ada, appearing in March 1985.

One of the principle outcomes of our experiments on detecting deadness errors was the conception and design of a language for specifying a much wider class of tasking errors, called *task sequencing errors*. This language is called TSL, Task Sequencing Language. A paper on TSL has been accepted for presentation at the International Ada Conference in Paris, May 14 - 16, 1985.

Runtime monitoring tools for deadness errors can now be extended to check for sequences of task interactions specified by TSL statements. This gives them the capability to detect very subtle errors in Ada tasking programs. This kind of tool has many applications in testing and monitoring distributed systems, including for example, flight control systems, communication networks, and secure message systems.

Current work on this project is focused on the design and applications of TSL. Extension of the previous tools for runtime deadness monitoring to support use of TSL is in progress. All implementation is in Ada and is designed for possible integration into future Ada support environments.

2 Proposal for September 1985 - August 1986.

Proposed research for the next year is on the following projects:

1. *Application of TSL as a testing and debugging tool.* This involves use of TSL to formulate critical properties of actual distributed Ada tasking systems for testing them by runtime monitoring.

2. *Application of TSL as a specification language for design of distributed systems in Ada.* This involves use of TSL as a language extension of Ada to specify tasking activity of an Ada tasking system prior to implementation.

3. *Design and implementation of a TSL runtime monitor.*

4. *Theory of connected events in distributed systems.*

Project 1 is aimed at testing the design of TSL as a practical language for specifying erroneous behavior patterns in tasking programs. Practical examples of Ada systems are to be used for these studies, including for example, a distributed message network. Some redesign of TSL is expected to result from this study.

Project 2 is aimed at developing TSL as a new task specification language, somewhat higher level than Ada itself, but having compatible scope and visibility rules. This goes beyond the use of TSL as a testing and debugging language. TSL specifications should be transformable into Ada tasking bodies. Again, changes to TSL are expected to result.

Project 3 is aimed at implementing a runtime monitor for TSL. A design document outlining our current implementation design is included with this proposal. This design builds on previous packages developed for the deadness error monitor. It is intended eventually to run efficiently on distributed hardware.

Projects 1 - 3 depend on theoretical investigation of concepts related to uncertainty of information obtained from distributed systems at runtime, for example the concept of *connected events* described in the accompanying publications. This work will be pursued in project 4.

3 Budget September 30, 1985 - September 29, 1986.

Professor David Luckham	$ 14,077	
20%		
Senior Research Associate	7,845	
15%		
1 Ph.D. student	13,500	
50% Academic		
100% Summer		
Secretary	4,080	
17%		
Administrative Assistant	1,308	
	40,810	
SEL Engineering Support	898	
2.2%		
Subtotal	41,708	
Benefits		
25.4% through 8/31/86		
25.6% through 8/31/87	10,603	
Total Salaries & Benefits	$52,311	$52,311
Expendable materials and supplies		1,264
Postage, Xeroxing, telephone		2,107
Computer Charges		16,330
Travel - 2 East Coast Trips		3,324
Subtotal		75,336
University Overhead @ 69%		51,982
1 Year Total		127,318

END

FILMED

10-85

DTIC